

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-111727

(P2002-111727A)

(43) 公開日 平成14年4月12日 (2002.4.12)

(51) Int.Cl. ⁷	識別記号	F I	テマコード*(参考)	
H 0 4 L 12/56		G 0 6 F 12/00	5 3 7 Z	5 B 0 1 7
G 0 6 F 12/00	5 3 7	12/14	3 1 0 Z	5 B 0 8 2
12/14	3 1 0	13/00	3 5 1 Z	5 B 0 8 5
13/00	3 5 1	15/00	3 3 0 A	5 B 0 8 9
15/00	3 3 0	H 0 4 L 11/20	1 0 2 D	

審査請求 未請求 請求項の数11 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願2000-299556(P2000-299556)

(22) 出願日 平成12年9月29日 (2000.9.29)

(71) 出願人 000208891

ケイディーディーアイ株式会社

東京都新宿区西新宿二丁目3番2号

(72) 発明者 竹森 敬祐

埼玉県上福岡市大原2-1-15 株式会社

ケイディディ研究所内

(72) 発明者 田中 俊昭

埼玉県上福岡市大原2-1-15 株式会社

ケイディディ研究所内

(74) 代理人 100084870

弁理士 田中 香樹 (外1名)

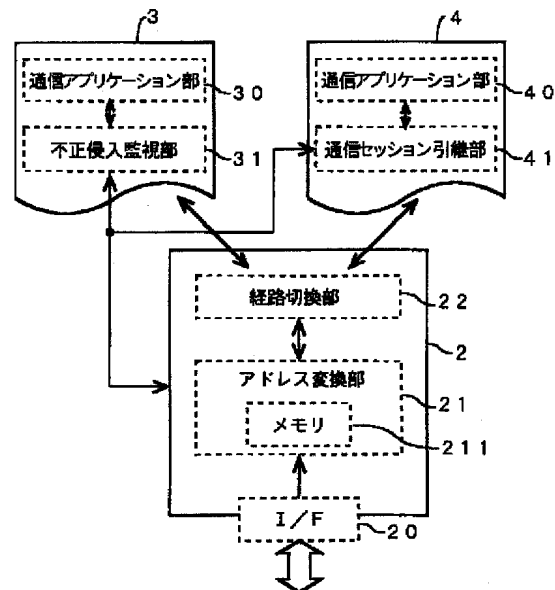
最終頁に続く

(54) 【発明の名称】 不正侵入防止システム

(57) 【要約】

【課題】 正規サーバへの不正侵入を防止し、かつ不正侵入者に不正侵入の失敗を悟られないようにした不正侵入防止システムを提供する。

【解決手段】 おとりサーバ4を正規サーバ3に併設し、正規サーバ3への不正侵入をおとりサーバ4へ導く不正侵入防止システムにおいて、正規サーバ3と外部端末5との間に確立された通信セッションが不正侵入に因るものであるか否かを判定する不正侵入監視部31と、不正侵入と判定された通信セッションを、正規サーバ3からおとりサーバ4に引継がせる通信セッション引継手段41と、不正侵入と判定された通信セッションにおいて、正規サーバ宛のデータ packets をおとりサーバに転送するルータ2とを具備した。



【特許請求の範囲】

【請求項1】 おとりサーバを正規サーバに併設し、前記正規サーバへの不正侵入を前記おとりサーバへ導く不正侵入防止システムにおいて、

前記正規サーバと外部端末との間に確立された通信セッションが不正侵入に因るものであるかを判定する不正侵入監視手段と、

不正侵入と判定された通信セッションを、正規サーバからおとりサーバに引継がせる通信セッション引継手段と、

前記不正侵入と判定された通信セッションにおいて、正規サーバ宛のデータパケットをおとりサーバに転送する経路切手手段とを具備したことを特徴とする不正侵入防止システム。

【請求項2】 前記おとりサーバから出力される応答パケットの内容を、前記正規サーバが前記データパケットを受信すれば出力するであろう応答パケットの内容に変換する応答変換手段をさらに具備したことを特徴とする請求項1に記載の不正侵入防止システム。

【請求項3】 前記おとりサーバは正規サーバのミラーサーバであることを特徴とする請求項1または2に記載の不正侵入防止システム。

【請求項4】 前記通信セッション引継手段は、正規サーバ宛のデータパケットと同一のデータパケットを前記おとりサーバへ順次転送する転送用バッファと、前記データパケットに応答して前記おとりサーバから返送された応答パケットを順次記憶する返送用バッファとを具備し、

前記返送用バッファは、前記不正侵入と判定された通信セッションがおとりサーバに引継がれると、引継後の最初のデータパケットに対応した応答パケットから順に出力することを特徴とする請求項1ないし3のいずれかに記載の不正侵入防止システム。

【請求項5】 前記通信セッション引継手段は、前記正規サーバ宛のデータパケットと同一のデータパケットを順次記憶する転送用バッファと、前記おとりサーバから返送された応答パケットを順次返送する返送用バッファとを具備し、前記転送用バッファは、前記不正侵入と判定された通信セッションがおとりサーバに引継がれると、引継後の最初のデータパケットから順に出力することを特徴とする請求項1ないし3のいずれかに記載の不正侵入防止システム。

【請求項6】 宛先が正規サーバからおとりサーバに変換されたデータパケットをおとりサーバへ転送せず、当該データパケットの応答パケットを疑似的に生成して返送する疑似応答手段を具備したことを特徴とする請求項1ないし5のいずれかに記載の不正侵入防止システム。

【請求項7】 不正侵入と判定された通信セッションの発信元アドレスを記憶し、次に当該発信元アドレスを有

するデータパケットが入力されると、おとりサーバとの間に通信セッションを確立することを特徴とする請求項1ないし6のいずれかに記載の不正侵入防止システム。

【請求項8】 前記おとりサーバとの間に確立された通信セッションにおいて、その行動ログないしは追跡データを収集することを特徴とする請求項1ないし7のいずれかに記載の不正侵入防止システム。

【請求項9】 おとりサーバを正規サーバに併設し、前記正規サーバへの不正侵入を前記おとりサーバへ導く不正侵入防止システムにおいて、

前記正規サーバを宛先とするデータパケットが、不正侵入者から送出されたものであるかを判定する不正侵入監視手段と、

不正侵入者から送出されたものと判定されたデータパケットをおとりサーバに転送する経路切手手段とを具備したことを特徴とする不正侵入防止システム。

【請求項10】 前記経路切手手段は、前記おとりサーバから出力される応答パケットの内容を、前記正規サーバが前記データパケットを受信すれば出力するであろう応答パケットの内容に変換する応答変換手段を含むことを特徴とする請求項9に記載の不正侵入防止システム。

【請求項11】 前記おとりサーバは正規サーバのミラーサーバであることを特徴とする請求項9または10に記載の不正侵入防止システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワーク上のデータ端末に悪意の第三者が不正侵入し、さらにはその内容を改竄、破壊等することを防止する不正侵入防止システムに係り、特に、不正侵入者に不正侵入の失敗を悟られること無く、これを確実に防止できる不正侵入防止システムに関する。

【0002】

【従来の技術】 近年、ホームページの改竄に代表される情報管理サーバへの不正侵入が後を立たない。このような問題点を解決するために、従来は、不正侵入者の通信セッションを情報管理サーバ内に侵入させない対策が講じられていた。例えば、情報管理サーバの不必要なポートを閉めることで攻撃されやすい経路を塞いだり、ファイアーウォールを設けて不正侵入者の通信セッションをフィルタリングしたり、あるいは不正侵入者の通信セッションを切断することなどが行われてきた。

【0003】 しかしながら、上記した従来の侵入防止システムでは、不正侵入者は侵入に失敗したことを認知できるため、他の侵入方法で再度侵入を試みたり、あるいは侵入を諦める代わりに大量の通信セッションを集中させ、サーバをダウンさせるなどの破壊工作や妨害工作に転じる場合があった。

【0004】 このような技術課題を解決するために、本来の情報管理サーバの近傍に、故意に侵入し易くしたお

とりサーバを配置し、当該おとりサーバでの改竄を許容することで、情報管理サーバへの不正侵入を防止すると共に、不正侵入者に不正侵入の失敗を悟られないようにした技術が提案されている（Network Associates社製のCyberCop Sting：米国）。

【0005】

【発明が解決しようとする課題】上記した従来技術では、サーバにおとり機能をインストールして仮想的なネットワークあるいはおとりサーバを作り出し、この仮想的なおとりサーバ等への通信設定を正規サーバよりも簡単10にすることで、不正侵入者をおとりサーバ等へおびき寄せていた。

【0006】しかしながら、前記おとり機能が作り出すおとりサーバ等は、その挙動が本来のサーバとは微妙に異なるために見破られてしまう可能性があった。このため、改めて正規サーバを攻撃されると、従来と同様に正規サーバへ侵入されてしまうという問題があった。

【0007】本発明の目的は、上記した従来技術の課題を解決し、正規サーバへの不正侵入を防止し、かつ不正侵入者に不正侵入の失敗を悟られないようにした不正侵入防止システムを提供することにある。20

【0008】

【課題を解決するための手段】上記した目的を達成するために、本発明は、おとりサーバを正規サーバに併設し、前記正規サーバへの不正侵入を前記おとりサーバへ導く不正侵入防止システムにおいて、前記正規サーバと外部端末との間に確立された通信セッションが不正侵入に因るものであるか否かを判定する不正侵入監視手段と、不正侵入と判定された通信セッションを、正規サーバからおとりサーバに引継がせる通信セッション引継手段と、前記不正侵入と判定された通信セッションにおいて、正規サーバ宛のデータ packets をおとりサーバに転送する経路切換手段とを具備したことを特徴とする。30

【0009】上記した特徴によれば、正規サーバとの間に確立された通信セッションが不正侵入に因るものと判定されると、当該通信セッションがおとりサーバに引継がれ、それ以後は、正規サーバ宛のデータ packets がおとりサーバに転送されるので、正規サーバを不正侵入から守ることができる。さらに、正規サーバとの間に確立された通信セッションがおとりサーバに引継がれるので、不正侵入者に不正侵入の失敗を悟られない。したがって、正規サーバを、同一の不正侵入者による更なる不正侵入行為、破壊行為あるいは迷惑行為等からも守ことができる。40

【0010】

【発明の実施の形態】以下、図面を参照して本発明を詳細に説明する。図1は、本発明の不正侵入防止システムが適用される通信ネットワークの構成を示したブロック図である。

【0011】通信ネットワーク1には、複数の通信端末50

5と共に、悪意の第三者による不正侵入から保護すべき正規サーバ3と、前記正規サーバ3に対する不正アクセスを身代わりとなって受け入れるおとりサーバ4とが、経路切換装置としてのルータ2（あるいはスイッチングハブ、帯域制御装置等）を介して接続されている。前記おとりサーバ4は正規サーバ3のミラーサーバとしての機能を有する。

【0012】図2は、前記ルータ2、正規サーバ3およびおとりサーバ4の構成を示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【0013】ルータ2において、ネットワークインターフェース（I/F）20は、当該ルータ2と通信ネットワーク1との物理的な接続を制御する。アドレス変換部21は、例えばNAT（Network Address Translator）としての機能を具備し、メモリ211に記憶されたアドレス対応情報に基づいて、入出力されるデータパケットのアドレス情報を書き換える。前記メモリ211に記憶された前記アドレス対応情報は、後述する正規サーバ3の不正侵入監視部31からの書き換え指示により書き換えられる。経路切換部22は、入力されたデータパケットを、その宛先アドレスに基づいて、正規サーバ3またはおとりサーバ4、あるいはその双方へ転送する。

【0014】正規サーバ3において、通信アプリケーション部30は、入力されたデータパケットに登録されているコマンドを実行する。不正侵入監視部31（例えば、Internet Security Systems社製のReal Secure：米国）は、パスワードが設定されているときに、その間違え回数が基準値を越えたアクセスや、ポートスキャンを実行したアクセス等を不正侵入者によるアクセスと判定し、その旨を前記通信アプリケーション部30、ルータ2および後述する通信セッション引継部41へ通知する。

【0015】おとりサーバ4において、その主要部である通信アプリケーション部40は、入力されたデータパケットに登録されているコマンドを、前記正規サーバ3の通信アプリケーション部30と同様に実行する。通信セッション引継部41は、後に詳述するように、不正侵入者と正規サーバ3との通信セッションを正規サーバ3から引継いで継続させる。

【0016】図3、4は、本発明におけるデータパケットの転送経路を模式的に示した図であり、図3は、正規利用者あるいは不正侵入と判定されるまでの不正侵入者による通信セッションを示し、図4は、不正侵入と判定された以降の不正侵入者による通信セッションを示している。

【0017】図5は、本発明における通信シーケンスの第1実施形態を示した図であり、ここでは、正規サーバ3の通信アプリケーション部30とおとりサーバ4の通信アプリケーション部40とが同期して動作する。

【0018】図3に示したように、正規利用者または不正

正侵入者が、いずれかの通信端末5から正規サーバ3のアドレスを指定してデータパケットを送出すると、ルータ2の経路変換部22は、受信したデータパケットを正規サーバ3〔図5(a)〕およびおとりサーバ4〔同図(b)〕の双方へ転送する。

【0019】正規サーバ3では、通信アプリケーション部30が前記データパケットを受信し、前記通信端末5との間に通信セッションを確立させる。通信アプリケーション部30は、データパケットに登録されているコマンドを実行して応答パケットを出力〔同図(c)〕する。この応答パケットは、ルータ2を経由して発信元の通信端末5へ返送される。不正侵入監視部31は、入力されるデータパケットを監視〔同図(d)〕し、前記通信端末5の利用者が不正侵入者であるか否かを判定する。

【0020】これと平行して、おとりサーバ4の通信セッション引継部41では、図3に示したように、ルータ2から転送されたデータパケットが転送用バッファ411に格納(バッファリング)され〔図5(e)〕、おとりサーバ4の通信アプリケーション部40へ転送〔同図(f)〕される。

【0021】通信アプリケーション部40は、入力されたデータパケットに登録されているコマンドを実行し、その応答パケットを生成して通信セッション引継部41へ返送〔同図(g)〕する。当該応答パケットは、通信セッション引継部41の返送用バッファに412に格納〔同図(h)〕されるが、この時点ではルータ2に対して返送されない。

【0022】当該通信セッションが正規利用者によるものであり、不正侵入監視部31により不正侵入が検知されなければ、上記した各処理が繰り返されることになる。

【0023】これに対して、当該通信セッションが不正侵入者によるものであり、これが前記不正侵入監視部31により検知されると、正規サーバ3の通信アプリケーション部30に対しては、通信アプリケーションを終了させるためのコマンドが通知〔同図(i)〕され、ルータ2および通信セッション引継部41に対しては、不正侵入を検知した旨が通知〔同図(j),(k)〕される。正規サーバ3の通信アプリケーション部30は、前記通知を検知すると、実行中の通信セッションを終了し、その旨を不正侵入監視部31へ通知〔同図(l)〕する。

【0024】通信セッション引継部41は、前記通知を、不正侵入と判定された最初のデータパケットのパケット番号と共に不正侵入監視部31から受信すると、図4に示したように、その返送用バッファ412に蓄積されている、前記パケット番号に対応した応答パケットから順にルータ2へ出力〔図5(m)〕する。

【0025】このように、本実施形態では、おとりサーバ4に通信セッション引継部41を設け、不正侵入者に対する応答パケットを、不正侵入と判定された最初のデ

ータパケットから順に出力するようにしたので、不正侵入者と正規サーバ3との通信セッションをおとりサーバ4に正常に引継がせて継続させることができる。

【0026】ルータ2では、前記アドレス変換部21が、返送用バッファ412から出力された応答パケットの内容を、正規サーバ3がデータパケットを受信すれば出力するであろう応答パケットの内容に変換して返送〔同図(n)〕する。すなわち、応答パケットの発信元アドレスを、おとりサーバ4のアドレスから正規サーバ3のアドレスに変換し、応答パケットのコマンドを、正規サーバ3へのアクセスに正孔した旨のコマンドに変換する。

【0027】したがって、不正侵入者は発信元アドレスが正規サーバである応答パケットを受け取ることになるので、正規サーバ3への不正侵入者に失敗したことを認識できない。

【0028】これ以後は、当該通信セッション内で通信端末5から出力されるデータパケット〔同図(o)〕の宛先アドレスは、ルータ2のアドレス変換部21において、全ておとりサーバ4のアドレスに書き換えられるのでおとりサーバ4に転送〔同図(p)〕される。したがって、正規サーバ3への不正侵入を防止できる。さらに、おとりサーバ4から返送〔同図(q)〕される応答パケットも、ルータ2のアドレス変換部21において、その発信元アドレスを全て正規サーバ3のアドレスに書き換えられて出力〔同図(r)〕されるので、正規サーバ3への不正侵入者に失敗したことを不正侵入者に悟られない。

【0029】上記したように、本実施形態によれば、不正侵入と判定された通信セッションのデータパケットは、その宛先アドレスを正規サーバのアドレスからおとりサーバのアドレスへ書き換えられるので、正規サーバ3への侵入を防止できる。また、不正侵入者はおとりサーバ4に侵入しているにもかかわらず、正規サーバ3への侵入に成功したものと勘違いし、比較的長時間にわたって接続を維持するので、その間を利用して行動ログや追跡データの収集が可能になる。さらに、不正侵入者には正規サーバ3への侵入に失敗したことを悟られないので、この不正侵入者による再度の侵入行為や他の妨害行為、破壊行為、迷惑行為等を防止できる。

【0030】図6は、本発明による通信シーケンスの第2実施形態を示した図である。上記した第1実施形態では、正規サーバ3の通信アプリケーション部30とおとりサーバ4の通信アプリケーション部40とが同期していたが、本実施形態では両者が非同期に動作し、おとりサーバ4は、不正侵入監視部31により不正侵入が検知されてからデータパケットを読み込んでコマンドを実行する。

【0031】図3に示したように、正規利用者または不正侵入者が、いずれかの通信端末5から正規サーバ3のアドレスを指定してデータパケットを送出すると、ルー

タ2の経路変換部22は、受信したデータパケットを、正規サーバ3〔図6(a)〕およびおとりサーバ4〔同図(b)〕の双方へ転送する。

【0032】正規サーバ3では、通信アプリケーション部30が前記データパケットを受信し、前記通信端末5との間に通信セッションを確立させる。通信アプリケーション部30は、データパケットに登録されているコマンドを実行して応答パケットを出力〔同図(c)〕する。この応答パケットは、ルータ2を経由して発信元の通信端末5へ返送される。不正侵入監視部31は、入力されるデータ

パケットを監視〔同図(d)〕し、前記通信端末5の利用者が不正侵入者であるか否かを判定する。

【0033】これと平行して、おとりサーバ4の通信セッション引継部41では、ルータ2から転送されたデータパケットが転送用バッファ411に格納〔同図(e)〕されるが、通信アプリケーション部40へは転送されない。当該通信セッションが正規利用者によるものであれば、上記した各処理が繰り返されることになる。

【0034】これに対して、当該通信セッションが不正侵入者によるものであり、これが前記不正侵入監視部31により検知されると、通信アプリケーション部30に対しては、通信アプリケーションを終了するコマンドが通知〔同図(i)〕され、ルータ2および通信セッション引継部41に対しては、不正侵入を検知した旨が通知〔同図(j),(k)〕される。

【0035】正規サーバ3の通信アプリケーション部30は、前記通知を検知すると実行中の通信セッションを終了する。通信セッション引継部41は、不正侵入が検知された旨を、当該不正侵入と判定された最初のデータパケットのパケット番号と共に受信し、その送信用バッファ412にバッファリングされている、当該パケット番号に対応したデータパケットから順におとりサーバ4の通信アプリケーション部40へ転送〔同図(f)〕する。

【0036】通信アプリケーション部40は、当該データパケットに登録されているコマンドを実行して応答パケットを生成し、これを通信セッション引継部41へ返送〔同図(g)〕する。当該応答パケットは、通信セッション引継部41を介してルータ2へ転送〔同図(m)〕される。ルータ2では、前記アドレス変換部21が応答パケットの内容を、正規サーバ3がデータパケットを受信すれば出力するであろう応答パケットの内容に変換して返送〔同図(n)〕する。

【0037】これ以後は、当該通信セッション内で通信端末5から出力されるデータパケット〔同図(o)〕の宛先アドレスは、ルータ2のアドレス変換部21において全ておとりサーバ4のアドレスに書き換えられるので、正規サーバ3への不正侵入を防止できる。さらに、おとりサーバ4から不正侵入者に返送される応答パケット

〔同図(q)〕の発信元アドレスも、ルータ2のアドレス

変換部21において全て正規サーバ3のアドレスに書き換えられるので、正規サーバ3への不正侵入者に失敗したことを不正侵入者に悟られない。

【0038】なお、上記した各実施形態では、不正侵入監視部31を正規サーバ3内に設け、通信セッション引継部41をおとりサーバ4内に設けるものとして説明したが、本発明はこれのみに限定されるものではなく、正規サーバ3およびおとりサーバ4の各通信アプリケーション部30、40と通信ネットワーク1との間であれば、どのような形態で設けても良い。

【0039】さらに、上記した各実施形態では、不正侵入と判定されたセッションのデータパケットは全ておとりサーバ4へ転送するものとして説明したが、データの消去コマンドのように、おとりサーバ4の機能を喪失させるような危険なコマンドを含むデータパケットに関しては、おとりサーバ4へも侵入させないことが望ましい。

【0040】そこで、本実施形態では、図7に示したように、サーバ4の機能を喪失させるような危険なデータパケットはおとりサーバ4の通信アプリケーション部40へ転送せず、通信セッション引継部41が応答パケットを生成・返送して疑似的に応答〔同図(s)〕し、さらには、ルータ2のアドレス変換部21において、その発信元アドレスを全て正規サーバ3のアドレスに書き換えて出力〔同図(x)〕する。このような構成によれば、おとりサーバ4を、その機能を喪失させるような危険な不正行為から守ることができる。

【0041】さらに、上記した各実施形態では、通信端末5からのアクセスに対して、最初は正規サーバ3との間に通信セッションを確立し、不正侵入が検知された時点で、当該通信セッションをおとりサーバ4に引継がせるものとして説明したが、不正侵入と判定されたアクセスの発信元アドレスを全て記憶しておき、次に同一の発信元アドレスを有するアクセスが検知された場合には、その通信セッションを最初からおとりサーバ4との間に確立させるようにしても良い。

【0042】

【発明の効果】本発明によれば、以下のような効果が達成される。

- (1) 正規サーバとの間に確立された通信セッションが不正侵入に因るものと判定されると、当該通信セッションがおとりサーバに引継がれ、それ以後は、正規サーバ宛のデータパケットが全ておとりサーバに転送されるので、正規サーバを不正侵入から守ることができる。
- (2) 不正侵入者はおとりサーバに侵入しているにもかかわらず、正規サーバへの侵入に成功したものと勘違いし、データを改竄あるいは破壊する。このため、不正侵入者は比較的長時間にわたって接続を維持するので、その間を利用して行動ログや追跡データの収集が可能になり、その結果、不正侵入者の特定が可能になる。

(3) 不正侵入者には、正規サーバへの侵入に失敗したことを悟られないので、この不正侵入者による再度の侵入行為、あるいは他の妨害行為や破壊行為等を防止できる。

(4) おとりサーバの機能を喪失させ得る危険なコマンドについては、おとりサーバへ転送することなく、疑似的に応答するようにしたので、おとりサーバの機能喪失を防止できるようになる。

【図面の簡単な説明】

【図1】 本発明の不正侵入防止システムが適用される 10
ネットワークの構成を示したブロック図である。

【図2】 図1の主要部の構成を示したブロック図である。

【図3】 本発明におけるデータパケットおよび応答パケットの流れ（不正侵入検知前）を示した図である。

【図4】 本発明におけるデータパケットおよび応答パケットの流れ（不正侵入検知後）を示した図である。

【図5】 第1実施形態の通信シーケンスを示した図である。

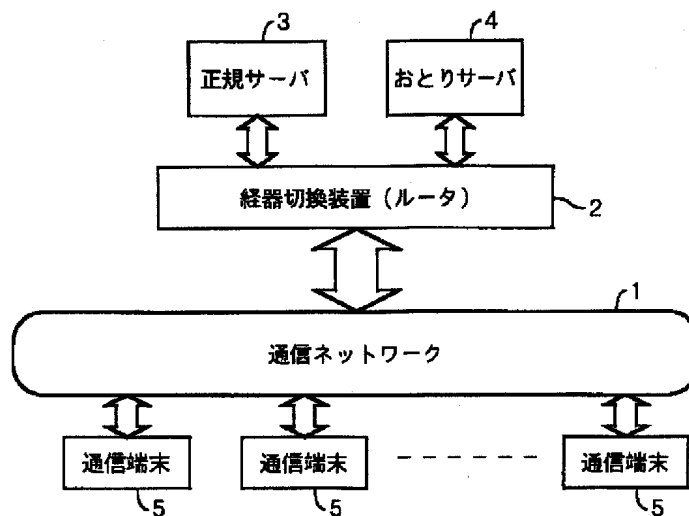
【図6】 第2実施形態の通信シーケンスを示した図である。

【図7】 第3実施形態の通信シーケンスを示した図である。

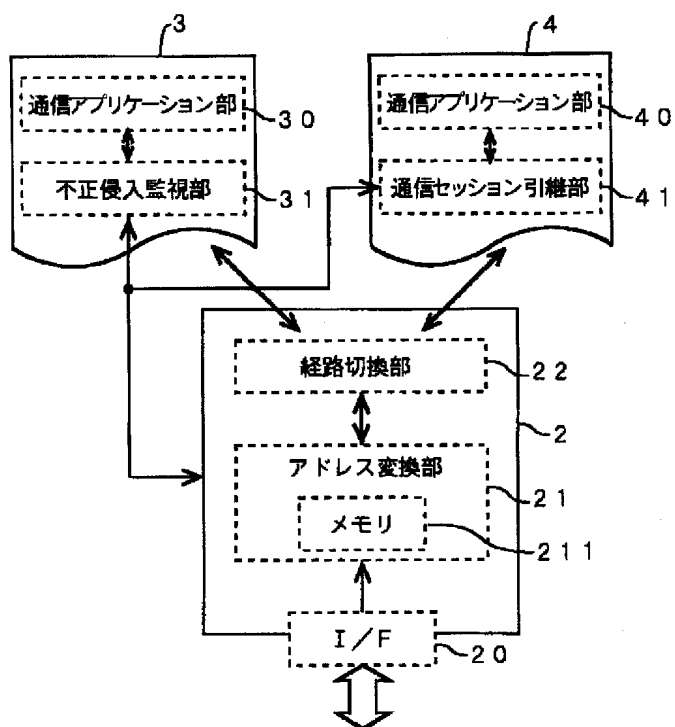
【符号の説明】

1…通信ネットワーク、2…ルータ、3…正規サーバ、4…おとりサーバ、5…通信端末、20…ネットワークインターフェース、21…アドレス変換部、22…経路切換部、31…不正侵入監視部、41…通信セッション引継部

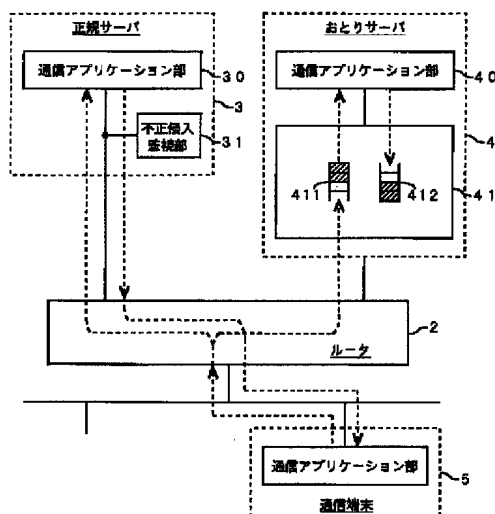
【図1】



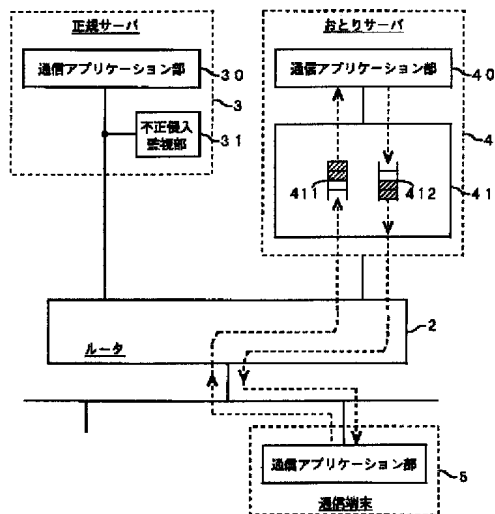
【図2】



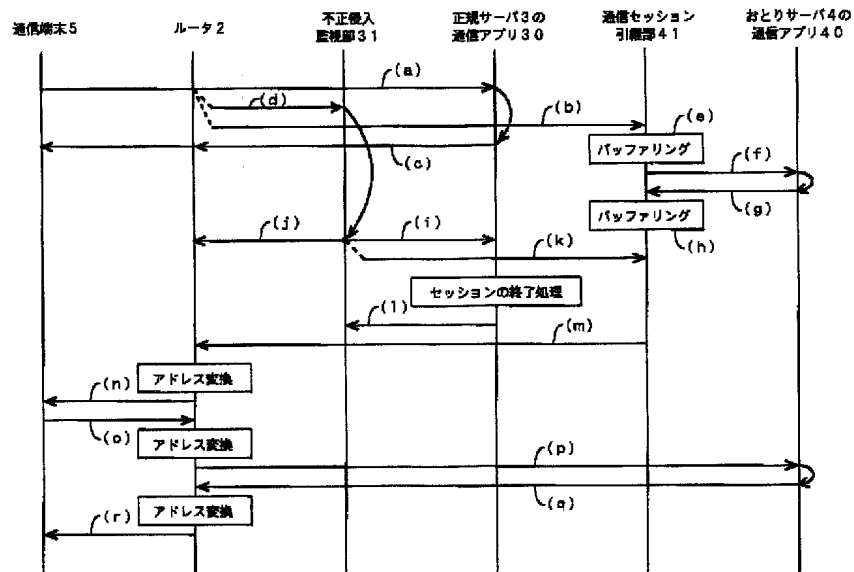
【図3】



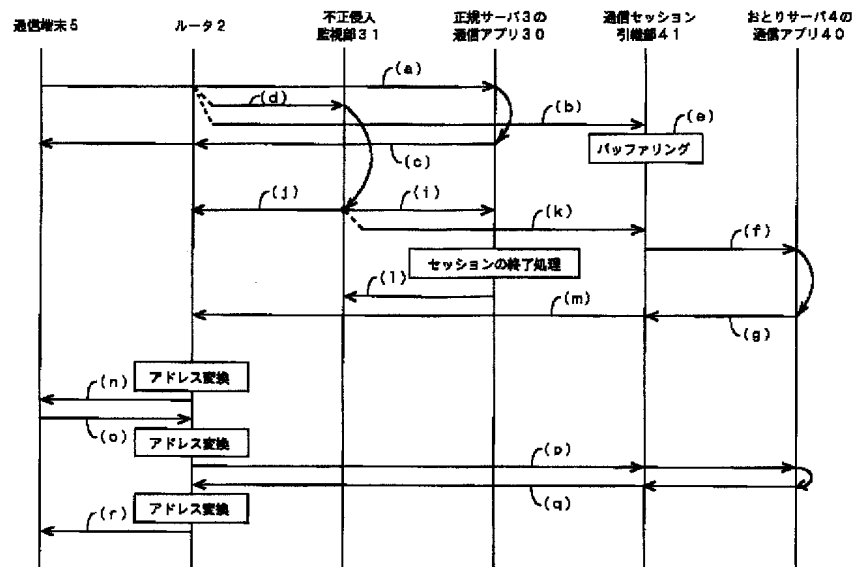
【図4】



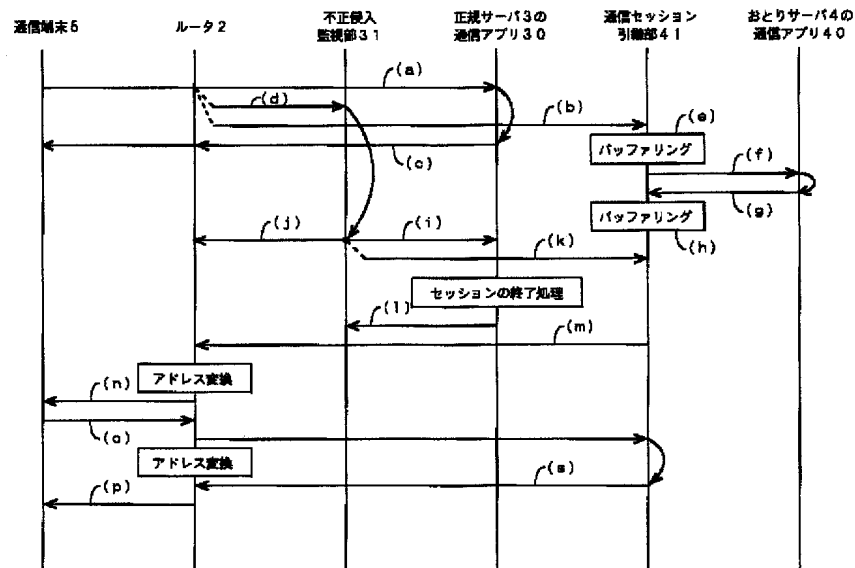
【図5】



【図6】



【図7】



フロントページの続き

(51) Int.Cl.⁷
H 0 4 L 12/22

識別記号

F I
H 0 4 L 11/26

メモード (参考)

(72) 発明者 中尾 康二
埼玉県上福岡市大原2-1-15 株式会社
ケイディディ研究所内

F ターム (参考) 5B017 AA01 BA06 BB09 CA15 CA16
5B082 EA11 FA11 GA11
5B085 AA01 AE00
5B089 GA19 GB01 GB02 KA17 KE02
KG03